The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
8/11/2009

SUBJECT:
Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution (MS09-038)

OVERVIEW:
Two vulnerabilities have been discovered in the way Microsoft Windows processes specially crafted Audio Visual Interleave (AVI) files. AVI is a common multimedia file format, consisting of audio and video data as well as instructions for displaying this data. These vulnerabilities can be exploited by opening a malicious AVI file received as an email attachment, or by visiting a web site that is hosting the file. Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in denial-of-service conditions.

SYSTEMS AFFECTED:

Microsoft Windows 2000 Service Pack 4
Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3
Microsoft Windows XP Professional x64 Edition Service Pack 2
Microsoft Windows Server 2003 Service Pack 2
Microsoft Windows Server 2003 x64 Edition Service Pack 2
Microsoft Windows Server 2003 with SP2 for Itanium-based Systems
Microsoft Windows Vista
Microsoft Windows Vista Service Pack 1
Microsoft Windows Vista Service Pack 2
Microsoft Windows Vista x64 Edition
Microsoft Windows Vista x64 Edition Service Pack 1
Microsoft Windows Vista x64 Edition Service Pack 2
Microsoft Windows Server 2008 for 32-bit Systems Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft Windows Server 2008 for x64-based Systems
Microsoft Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft Windows Server 2008 for Itanium-based Systems
Microsoft Windows Server 2008 for Itanium-based Systems Service Pack 2

RISK:

Government:
Large and medium government entities: High
Small government entities: High

Businesses:
Large and medium business entities: High
Small business entities: High

Home users: High

DESCRIPTION:
Two vulnerabilities have been discovered in the way Microsoft Windows processes AVI files. AVI is a common multimedia file format, consisting of audio and video data as well as instructions for displaying this data. The vulnerabilities are caused by the Windows operating system failing to properly handle AVI files with malformed headers. The specially crafted AVI file may be received via an email attachment or hosted on a Web site.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:
Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
Remind users not to download or open files from un-trusted websites.
Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
If you believe you have been affected by attacks exploiting this vulnerability, please contact us immediately.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/Bulletin/ms09-038.mspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1545
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1546

Security Focus:
http://www.securityfocus.com/bid/35967
http://www.securityfocus.com/bid/35970